UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/733,320	12/12/2003	Robert Joseph Harley	021185-000200US	9086

20350 7590 12/23/2008
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
12/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/733,320	12/12/2003	Robert Joseph Harley	021185-000200US	9086

20350 7590 10/09/2008
TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
10/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/733,320	HARLEY, ROBERT JOSEPH	
	Examiner	Art Unit	
	CARLTON V. JOHNSON	2136	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 June 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date *7-25-2008*.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This action is responding to application papers filed on **12-12-2003**.

2. Claims **1 - 15** are pending. Claims **1, 8, 10 - 15** have been amended. Claims **1, 12, 15** are independent.

Response to Arguments

3. Applicant's arguments filed 6/30/2008 have been fully considered and they were partially persuasive and new grounds of rejection have been entered.

Responses:

3.1 The amendments submitted as part of the advisory action dated 6-18-2008 and not entered at that time will be considered to constitute the set of amendments Applicant wishes to submit for the Request for Continued Examination (RCE) dated 6-30-2008 and the basis for this Office Action. No amendments were submitted with the RCE.

3.2 The FOUQUET reference as part of an IDS discloses the process of counting the number of points on an elliptical curve and the capability to lift (canonical lift) an equation and operate with p-adic numbers.

Applicant has stressed that the amount of time required to perform cryptographic calculations has been greatly reduced due to applicant's invention. Applicant has stated that the Satoh algorithms (FOUQUET reference) previously reduced the time required for cryptographic calculations and that the claimed invention reduces the time

even further. Applicant's invention discloses: counting points on an elliptic curve; canonical lifting of an equation; and recursive operations. These are all pre-existing algorithmic operations. Is it applicant's position that the reduction in time is what constitutes the invention?

3.3 The Hoffstein prior art discloses calculations with Frobenius equations and elliptic curves. (see Hoffstein col. 3, lines 59-62: Frobenius operation on elliptic curves; col. 8, lines 7-11: using elliptic curves) Applicant argues that it is not the same type of operations but the Holstein reference does discloses operations performed on elliptic curves.

The claimed invention is partially directed to Frobenius equations, which are disclosed in the Hoffstein prior art. In addition, the claimed invention is also partially directed toward mathematical calculations using elliptic curves, which is disclosed in the Gressel prior art. The Gressel prior art is not used to reject claim limitations addressing computations using Frobenius equations.

3.4 The claim limitations recite arithmetic operations which are performed on integer values using mathematical algorithms. The Hoffstein, Fouquet, Gressel and Penner prior art references disclose arithmetic operations performed on integer values including operations such as partial result operations, multiplication operations, and register usage.

The Hoffstein prior art discloses arithmetic operations using elliptic curves and

Frobenius equations. The Gressel prior art discloses the results of a first arithmetic operation used as input to another arithmetic operation such as a first and second partial result combined to generate a final result.

The FOUQUET (Satoh) prior art discloses operations for counting points on an elliptic curve, canonical lift of an equation, and operations on p-adic numbers.

And, the Gressel prior art discloses partial results from an arithmetic operation. (see Gressel col. 2, lines 31-37: arithmetic operations utilizing partial results from previous multiplication (operations)) In addition, the Gressel prior art discloses storing and utilizing the results of a previous operation in subsequent arithmetic operations. (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into a next (subsequent) operation)

The Penner prior art discloses performing canonical lift calculations, Teichmuller calculations, recursive operations, and error type algorithmic arithmetic operations.

Claim Rejections – 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. The claimed invention is directed to non-statutory subject matter. Claims **14, 15** are rejected as directed toward non-statutory subject matter. Claims **14, 15** are claiming: "logic for receiving"; "logic for determining"; "logic for identifying"; and some mathematical computations without having any hardware elements in the claim for

performing the functions that have been claimed. There is no disclosure that the claim limitations for "logic for receiving", "logic for determining" and "logic for identifying" are hardware implementations. Therefore, claim limitations for Claims **14, 15** are strictly software implementations and directed toward non-statutory matter.

Applicant stated that it is not clear what is meant by "a strictly software implementation". In paragraph [0040] of the specification discloses: "Steps or functions described herein can be performed in hardware, **software** or a combination of the two." The specification must be interpreted in the broadest sense. In the broadest sense, based on the above specification disclosure, the invention can be embodied in software only or "a strictly software implementation". A strictly software implementation is directed toward non-statutory subject matter. Claims **14, 15** can be interpreted as a strictly software implementation and directed toward non-statutory matter. Therefore, the logic in claims 14, 15 can be interpreted as being embodied in software only.

Claims **1 - 9, 11, 12, 14** are directed toward non-statutory subject matter. Independent claims **1, 12, 14** recite a method for performing a mathematical function. To satisfy 101 requirements, the claim must be for a practical application of the Section 101 judicial exception. Since there is no physical transformation in order to establish a practical application, a useful, concrete and tangible result appears to be lacking. Dependent claims **10, 15** recite the limitation generating a cryptographic key which is a useful, concrete and tangible result. Perhaps these claim limitations should be moved to the independent claims.

Appropriate correction required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims **12, 13** are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The terms "total" and "entire" do not appear within the specification or the original claims. The specification discloses the process of counting the number of points on a curve but does not specify a precise upper limit for the number of points such as "total" and length of a curve for point counting such as "entire".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 103 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an

application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims **1 - 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Hoffstein et al.** (US Patent No. **7,031,468**) in view of **Gressel et al.** (US Patent No. **6,748,410**) and further in view of **Penner** (US Patent No. **7,158,569**) and further in view of **FOUQUET** ("An Extension of FOUQUET's Algorithm and Its Implementation").

Regarding Claim 1, Hoffstein discloses a computer-implemented method for computing the number of points on an elliptic curve the method comprising:

a) receiving an elliptic curve having a <u>total</u> number of points on the <u>entire</u> curve; (see Hoffstein col. 3, lines 59-62: Frobenius operation on elliptic curves; col. 8, lines 7-11: using elliptic curves; col. 3, lines 7-9: computer system; software, computer implemented) and (FOUQUET Section 1.2, lines 5-18: count number of points on an elliptic curve; lifted equation)

   There is no disclosure for total number of points on an elliptic curve.

b) determining the <u>total</u> number of points on the elliptic curve, wherein the determining includes solving a lifted Frobenius equation to a full precision by using first and second parts with a reduced precision, (see Hoffstein col. 3, lines 59-62; col. 8, lines 7-11: Frobenius operation on elliptic curves utilizing elliptic curves; col. 1, lines 56-59: computation using a number of points on elliptic curves over a finite field; elliptic curve defined by a group of points; a

computation used to) and (FOUQUET Section 1.2, lines 5-18: count number of points on an elliptic curve; lifted equation)

There is no disclosure for total number of points on an elliptic curve.

wherein the solving includes:

a) computing to the reduced precision, said first part firstly computes a first partial solution of said lifted Frobenius equation using said first part recursively, (see Hoffstein col. 3, lines 59-62: Frobenius operation on elliptic curves; col. 8, lines 7-11: utilizing elliptic curves) and (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 3, lines 28-32; col. 11, lines 7-11; col. 11, lines 40-49: arithmetic operation or instructions) and (see Penner col. 20, lines 11-16: recursive operations)

b) applying a Frobenius operation to said first partial solution, (see Hoffstein col. 3, lines 59-62: Frobenius operation on elliptic curves; col. 8, lines 7-11: utilizing elliptic curves)

c) computing an error term/correction factors for said lifted Frobenius equation; computing correction factors for said lifted Frobenius equation, (see Hoffstein col. 3, lines 59-62: Frobenius operation on elliptic curves; col. 8, lines 7-11: utilizing elliptic curves) and (see Penner col. 20, lines 8-11: error terminate)

d) computing, to the reduced precision (see Penner col. 1, lines 62-63: precision algorithmic operations), a second partial solution of a modified lifted Frobenius equation that includes the error term and the correction factors

(see Hoffstein col. 3, lines 59-62: Frobenius operation on elliptic curves; col. 8, lines 7-11: utilizing elliptic curves) using said second part (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation)

wherein computing the second partial solution includes:

e) computing, to the reduced precision, a third partial solution of said modified lifted Frobenius equation using said second part recursively (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 3, lines 28-32; col. 11, lines 7-11; col. 11, lines 40-49: arithmetic operation or instructions) and (see Penner col. 20, lines 11-16: recursive operations)

f) applying a Frobenius operation to said third partial solution, (see Hoffstein col. 3, lines 59-62: Frobenius operation on elliptic curves; col. 8, lines 7-11: utilizing elliptic curves) and (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 7, lines 28-33: col. 26, lines 6-26: partial result algorithmic operations)

g) updating said error term, (see Penner col. 20, lines 8-11: error terminate)

h) computing, to the reduced precision, a fourth partial solution of said modified lifted Frobenius equation using said second part recursively (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 7, lines 28-33: col. 26,

lines 6-26: partial result algorithmic operations) and (see Penner col. 20, lines 11-16: recursive operations)

i) combining said third partial solution and said fourth partial solution to create the second partial solution, (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 7, lines 28-33: col. 26, lines 6-26: partial result algorithmic operations)

f) combining said first partial solution and said second partial solution to provide the solution at the full precision (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 7, lines 28-33: col. 26, lines 6-26: partial result algorithmic operations)

Gressel discloses partial (first, second) algorithmic operations in the mathematical calculations used to generate a cryptographic key.

It would have been obvious to one of ordinary skill in the art to modify Hoffstein to perform partial algorithmic operations in the generation of a cryptographic key as taught by Gressel. One of ordinary skill in the art would have been motivated to employ the teachings of Gressel in order to enable the capability to provide for accelerating and securing improved methods for modular and exponentiation algorithmic operations. (see Gressel col. 1, lines 39-45: " ... *The present invention seeks to provide improved apparatus and methods for modular multiplication and exponentiation and for serial integer division, and for accelerating and securing*

modular arithmetic processors and accelerating memory transfers to computer peripheral that need simplified accelerated memory to peripheral data transfers with limited CPU core changes. ... ")

FOUQUET discloses canonical lift. (see FOUQUET Section 1.2, lines 5-18; Section 1.4, lines 19-29: lift of an equation)

It would have been obvious to one of ordinary skill in the art to modify Hoffstein to compute a trace for as taught by FOUQUET. One of ordinary skill in the art would have been motivated to employ the teachings of FOUQUET in order to a relatively fast algorithm for counting points on elliptic curves. (see FOUQUET page 1)

Penner discloses Teichmuller lift of a given finite-field polynomial, recursive operations, and precision algorithmic operations.

It would have been obvious to one of ordinary skill in the art to modify Hoffstein to enable the capability to perform canonical, Teichmuller, recursive, and error type algorithmic operations as taught by Penner. One of ordinary skill in the art would have been motivated to employ the teachings of Penner in order to enable the capability to provide new, novel, and efficient methods for calculating algorithmic transform operations. (see Penner col. 1, lines 52-55: " ... *In combination with these wavelet filters, the invention also provides new methods for calculating various classical transforms including the Fourier transform and its inverse. This*

immediately provides novel and efficient methods for digital filtering. ... ")

Regarding Claim 2, Hoffstein discloses the method of claim 1. (see Hoffstein col. 3, lines 59-62: Frobenius operation on elliptic curves; col. 8, lines 7-11: utilizing elliptic curves; col. 3, lines 54-56: finite field polynomial operations) Hoffstein does not specifically disclose reduced precision is one half of said given full precision. However, Penner discloses in which said reduced precision is one half of said given full precision. (see Penner col. 1, lines 62-63: precision algorithmic operations)

It would have been obvious to one of ordinary skill in the art to modify Hoffstein to perform precision algorithmic operations as taught by Penner. One of ordinary skill in the art would have been motivated to employ the teachings of Penner in order to enable the capability to provide new, novel, and efficient methods for calculating algorithmic transform operations. (see Penner col. 1, lines 52-55)

Regarding Claim 3, Hoffstein discloses the method of claim 1. (see Hoffstein col. 3, lines 59-62: col. 8, lines 7-11; col. 3, lines 54-56: Frobenius operation on elliptic curves; finite field polynomial operations)

Gressel discloses computations using said first and second parts. (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 3, lines 28-32; col. 11, lines 7-11; col. 11, lines 40-49: arithmetic operation or instructions)

FOUQUET discloses canonical lift of an equation. (see FOUQUET Section 1.2, lines 5-18; Section 1.4, lines 19-29: lift of an equation)

It would have been obvious to one of ordinary skill in the art to modify Hoffstein to compute a trace for as taught by FOUQUET. One of ordinary skill in the art would have been motivated to employ the teachings of FOUQUET in order to a relatively fast algorithm for counting points on elliptic curves. (see FOUQUET page 1)

Penner discloses computing the Teichmuller operations of a given finite-field polynomial. (see Penner col. 26, line 31: Teichmuller lift of a given finite-field polynomial)

It would have been obvious to one of ordinary skill in the art to modify Hoffstein to perform Teichmuller type algorithmic operations as taught by Penner. One of ordinary skill in the art would have been motivated to employ the teachings of Penner in order to enable the capability to provide new, novel, and efficient methods for calculating algorithmic transform operations. (see Penner col. 1, lines 52-55)

Regarding Claim 4, Hoffstein discloses the method of claim 1 on said elliptic curves. (see Hoffstein col. 3, lines 59-62: col. 8, lines 7-11; col. 3, lines 54-56: Frobenius operation on elliptic curves; finite field polynomial operations) Hoffstein does not specifically disclose canonical lift. However, FOUQUET discloses in which said first and second parts compute the canonical lift. (see FOUQUET Section 1.2, lines 5-18; Section 1.4, lines 19-29: count points on elliptic curve; canonical lift)

It would have been obvious to one of ordinary skill in the art to modify Hoffstein to compute a trace for as taught by FOUQUET. One of ordinary skill in the art would have been motivated to employ the teachings of FOUQUET in order to a relatively fast algorithm for counting points on elliptic curves. (see FOUQUET page 1)

Regarding Claim 5, Hoffstein discloses the method of claim 1 of a given finite-field element. (see Hoffstein col. 3, lines 59-62: col. 8, lines 7-11; col. 3, lines 54-56: Frobenius operations on elliptic curves; finite field polynomial operations) Hoffstein does not disclose said first and second parts compute the multiplicative representative. However, Gressel discloses in which said first and second parts compute the multiplicative representative. (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 3, lines 28-32; col. 11, lines 7-11; col. 11, lines 40-49: arithmetic operation or instructions; col. 2, lines 31-37: multiplication operations; col. 29, lines 43-49: representation of numbers)

It would have been obvious to one of ordinary skill in the art to modify Hoffstein to perform partial algorithmic operations as taught by Gressel. One of ordinary skill in the art would have been motivated to employ the teachings of Gressel in order to enable the capability to provide for accelerating and securing improved methods for modular and exponentiation algorithmic operations. (see Gressel col. 1, lines 39-45)

Regarding Claim 6, Hoffstein discloses the method of claim 1. (see Hoffstein col. 1, lines 56-59: computing the number of points on elliptic curves over a finite field)

Hoffstein does not specifically disclose where said first and second parts compute the trace and a p-adic number. However, FOUQUET discloses wherein said first and second parts compute the trace or a p-adic number. (see FOUQUET Section 1.2, lines 19-25: p-adic precision; trace of Frobenius)

It would have been obvious to one of ordinary skill in the art to modify Hoffstein to compute a trace as taught by FOUQUET. One of ordinary skill in the art would have been motivated to employ the teachings of FOUQUET in order to a relatively fast algorithm for counting points on elliptic curves. (see FOUQUET page 1)

Regarding Claim 7, Hoffstein discloses the method of claim 1. (see Hoffstein col. 1, lines 56-59: computing the number of points on elliptic curves over a finite field) Hoffstein does not specifically disclose said first and second parts compute the norm and a p-adic number. However, FOUQUET discloses wherein said first and second parts compute the norm. (see FOUQUET Section 1.2, lines 5-18: norm (specification on page 2 defines norm as the count of the number of points))

It would have been obvious to one of ordinary skill in the art to modify Hoffstein to compute a trace for as taught by FOUQUET. One of ordinary skill in the art would have been motivated to employ the teachings of FOUQUET in order to a relatively fast algorithm for counting points on elliptic curves. (see FOUQUET page 1)

Regarding Claim 8, Hoffstein discloses the method of claim 10, further comprising: receiving a sequence of elliptic curves and determining the number of points on each

elliptic curve. (see Hoffstein col. 3, lines 59-62: col. 8, lines 7-11: Frobenius operation on elliptic curves; utilizing elliptic curves) Hoffstein does not specifically disclose where said first and second parts analyze the sequence. However, Gressel discloses wherein said first and second parts analyze the sequence. (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 3, lines 28-32; col. 11, lines 7-11; col. 11, lines 40-49: arithmetic operation or instructions)

It would have been obvious to one of ordinary skill in the art to modify Hoffstein to use said first and second parts to analyze the sequence using algorithmic operations as taught by Gressel. One of ordinary skill in the art would have been motivated to employ the teachings of Gressel in order to enable the capability to provide for accelerating and securing improved methods for modular and exponentiation algorithmic operations. (see Gressel col. 1, lines 39-45)

Regarding Claim 9, Hoffstein discloses the method of claim 8. using one of the secure elliptic curves. (see Hoffstein col. 3, lines 59-62: col. 8, lines 7-11; col. 3, lines 54-56: Frobenius operation on elliptic curves; finite field polynomial operations) Hoffstein does not specifically disclose wherein generating a cryptographic key for use in a digital processing system using one of the secure elliptic curves. However, Gressel discloses wherein generating in which said analysis generates a cryptographic key for use in a digital processing system using one of the secure elliptic curves. (see Gressel col. 3, lines 28-32: arithmetic operations utilized to generate cryptographic key(s); col. 3, lines

18-22: processor utilization for key generation)

It would have been obvious to one of ordinary skill in the art to modify Hoffstein to generate cryptographic key using algorithmic operations as taught by Gressel. One of ordinary skill in the art would have been motivated to employ the teachings of Gressel in order to provide for accelerating and securing improved methods for modular and exponentiation algorithmic operations. (see Gressel col. 1, lines 39-45)

Regarding Claims 10, 13, 15, Hoffstein discloses the method of claim 1, further comprising: based on the <u>total</u> number of points, identifying whether the elliptic curve is a secure elliptic curve. (see Hoffstein col. 3, lines 59-62: col. 8, lines 7-11; col. 3, lines 54-56: Frobenius operation on elliptic curves; finite field polynomial operations; col. 1, lines 56-59: computing the number of points on elliptic curves over a finite field) and (see FOUQUET Section 1.2, lines 5-18; Section 1.4, lines 19-29: count points on elliptic curve; canonical lift) Hoffstein does not specifically disclose generating a cryptographic key. However, Gressel discloses generating a cryptographic key. (see Gressel col. 3, lines 28-32: cryptographic key generation)

There is no disclosure for total number of points on an elliptic curve.

It would have been obvious to one of ordinary skill in the art to modify Hoffstein to compute a trace as taught by FOUQUET. One of ordinary skill in the art would have been motivated to employ the teachings of FOUQUET in order to a relatively fast algorithm for counting points on elliptic curves. (see FOUQUET page 1)

And, It would have been obvious to one of ordinary skill in the art to modify

Hoffstein to generate a cryptographic key as taught by Gressel. One of ordinary skill in the art would have been motivated to employ the teachings of Gressel in order to provide for accelerating and securing improved methods for modular and exponentiation algorithmic operations. (see Gressel col. 1, lines 39-45)

Regarding Claim 11, Hoffstein discloses the method of claim 1. (see Hoffstein col. 3, lines 59-62: col. 8, lines 7-11; col. 3, lines 54-56: Frobenius operation on elliptic curves; finite field polynomial operations) Hoffstein does not specifically disclose storing the <u>total</u> number of points on the elliptic curve in a memory. However, Gressel discloses storing the number of points on the elliptic curve in a memory of the computer. (see Gressel col. 41, lines 20-23: register (memory) usage; storage of parameters (points)) There is no disclosure for total number of points on an elliptic curve.

It would have been obvious to one of ordinary skill in the art to modify Hoffstein to store points in memory as taught by Gressel. One of ordinary skill in the art would have been motivated to employ the teachings of Gressel in order to provide for accelerating and securing improved methods for modular and exponentiation algorithmic operations. (see Gressel col. 1, lines 39-45)

Regarding Claims 12, 14, Hoffstein discloses a computer readable medium embodying program code, an integrated circuit for directing one or more processors to perform an operation for computing the number of points on an elliptic curve, the operation comprising the steps of:

a) receiving an elliptic curve having a <u>total</u> number of points on the <u>entire</u> curve; (see Hoffstein col. 1, lines 56-59: computations using the number of points on elliptic curves over a finite field) and (see FOUQUET Section 1.2, lines 5-18: compute the number of points on a elliptic curve)

There is no disclosure for total number of points on an elliptic curve.

b) determining a number of points on the elliptic curve, wherein the determining includes solving a lifted Frobenius equation to a full precision by using first and second parts with a reduced precision, (see Hoffstein col. 1, lines 56-59: computations using the number of points on elliptic curves over a finite field) and (see FOUQUET Section 1.2, lines 5-18: compute the number of points on a elliptic curve)

wherein the solving includes:

a) computing, to the reduced precision (see Penner col. 1, lines 62-63: precision algorithmic operations), a first partial solution of said lifted Frobenius equation (see Hoffstein col. 3, lines 59-62: Frobenius operation on elliptic curves; col. 8, lines 7-11: utilizing elliptic curves) using said first part (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 7, lines 28-33: col. 26, lines 6-26: partial result algorithmic operations) recursively (see Penner col. 20, lines 11-16: recursive operations),

b) applying a Frobenius operation to said first partial solution, (see Hoffstein col. 3, lines 59-62: Frobenius operation on elliptic curves; col. 8, lines 7-11:

utilizing elliptic curves) and (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 7, lines 28-33: col. 26, lines 6-26: partial result algorithmic operations)

c) computing an error term for said lifted Frobenius equation, (see Hoffstein col. 3, lines 59-62: Frobenius operation on elliptic curves; col. 8, lines 7-11: utilizing elliptic curves) and (see Penner col. 20, lines 8-11: error terminate)

d) computing correction factors for said lifted Frobenius equation, (see Hoffstein col. 3, lines 59-62: Frobenius operation on elliptic curves; col. 8, lines 7-11: utilizing elliptic curves) and (see Penner col. 20, lines 8-11: error terminate)

e) computing, to the reduced precision, a second partial solution of a modified lifted Frobenius equation that includes the error term and the correction factors using said second part, (see Hoffstein col. 3, lines 59-62: Frobenius operation on elliptic curves; col. 8, lines 7-11: utilizing elliptic curves) wherein computing the second partial solution includes:

   a) computing, to the reduced precision (see Penner col. 1, lines 62-63: precision algorithmic operations), a third partial solution of said modified lifted Frobenius equation using said second part recursively, (see Gressel col. 7, lines 28-33: col. 26, lines 6-26: partial result algorithmic operations) (see Penner col. 20, lines 11-16: recursive operations)

   b) applying a Frobenius operation to said third partial solution, (see Hoffstein col. 3, lines 59-62: Frobenius operation on elliptic curves; col. 8, lines 7-11: utilizing elliptic curves)

c) updating said error term, (see Penner col. 20, lines 8-11: error terminate)

a) computing, to the reduced precision, a fourth partial solution of said modified lifted Frobenius equation using said second part recursively, (see Gressel col. 7, lines 28-33: col. 26, lines 6-26: partial result algorithmic operations) and (see Penner col. 20, lines 11-16: recursive operations)

b) combining said third partial solution and said fourth partial solution to create the second partial solution, (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 3, lines 28-32; col. 11, lines 7-11; col. 11, lines 40-49: arithmetic operation or instructions)

f) combining said first partial solution and said second partial solution to provide the solution at the full precision. (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 3, lines 28-32; col. 11, lines 7-11; col. 11, lines 40-49: arithmetic operation or instructions)

Gressel discloses partial (first, second) algorithmic operations in the mathematical calculations to generate a cryptographic key.

It would have been obvious to one of ordinary skill in the art to modify Hoffstein to perform partial algorithmic operations in the generation of a cryptographic key as taught by Gressel. One of ordinary skill in the art would have been motivated to employ the teachings of Gressel in order to enable the capability to provide for

accelerating and securing improved methods for modular and exponentiation algorithmic operations. (see Gressel col. 1, lines 39-45)

And, FOUQUET discloses canonical lift. (see FOUQUET Section 1.2, lines 5-18: canonical lift of an equation)

It would have been obvious to one of ordinary skill in the art to modify Hoffstein to compute a trace as taught by FOUQUET. One of ordinary skill in the art would have been motivated to employ the teachings of FOUQUET in order to a relatively fast algorithm for counting points on elliptic curves. (see FOUQUET page 1)

In addition, Penner discloses Teichmuller lift of a given finite-field polynomial, recursive operations, and precision algorithmic operations.

It would have been obvious to one of ordinary skill in the art to modify Hoffstein to enable the capability to perform canonical, Teichmuller, recursive, and error type algorithmic operations as taught by Penner. One of ordinary skill in the art would have been motivated to employ the teachings of Penner in order to enable the capability to provide new, novel, and efficient methods for calculating algorithmic transform operations. (see Penner col. 1, lines 52-55)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-

270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136

Carlton V. Johnson
Examiner
Art Unit 2136

CVJ
September 15, 2008